## Amendments to the Claims

1    Claim 1 (currently amended):  A method of ~~improving~~ security policy administration and

2    enforcement ~~using a role-permission model~~ in a security system that controls access using

3    security objects, comprising steps of:

4         associating each of a plurality of roles with one of the security objects, each of the

5    security objects specifying at least one resource and for each resource, at least one action to be

6    permitted on the resource; and

7         controlling access, by a plurality of subjects, to the actions on the resources using the

8    security objects, wherein each of the subjects has been granted at least one of the roles.

9    ~~identifying one or more groups of permitted actions on selected resources;~~

10   ~~assigning a name to each identified group; and~~

11   ~~associating subjects with each assigned name.~~


Claim 2 (canceled)


1    Claim 3 (currently amended):  The method according to Claim 1, wherein at least one of the

2    selected resources [[are]] is an executable ~~methods~~ method.


1    Claim 4 (currently amended):  The method according to Claim 1, wherein at least one of the

2    selected resources ~~are columns~~ is a column of a database table.


1    Claim 5 (currently amended):  The method according to Claim 1, wherein at least one of the

2    ~~selected resources are rows~~ is a row of a database table.


1    Claim 6 (currently amended):  The method according to Claim 1, wherein at least one of the

2    ~~selected~~ resources ~~are files~~ is a file and the permitted actions on the at least one resource are file

3    access operations.


1    Claim 7 (currently amended):  The method according to Claim 1, wherein at least one of the

2    ~~selected~~ resources [[are]] is a function [[calls]] call to ~~functions~~ a function of ~~one or more~~ an

3    executable ~~programs~~ program.


1    Claim 8 (currently amended):  The method according to Claim 1, wherein at least one of the

2    ~~selected~~ resources [[are]] is an Enterprise JavaBean ("EJB") ~~JavaBeans ("EJBs")~~ and the

3    permitted actions on the at least one resource are methods on the [[EJBs]] EJB.


1    Claim 9 (currently amended):  The method according to Claim 1, wherein at least one of the

2    ~~selected~~ resources ~~are servlets~~ is a servlet and the permitted actions on the at least one resource

3    are methods of the ~~servlets~~ servlet.


1    Claim 10 (currently amended):  The method according to Claim 1, wherein at least one of the

2    ~~selected~~ resources [[are]] is a Uniform Resource Identifier ("URI") ~~Identifiers ("URIs")~~ and the

3    permitted actions on the at least one resource are methods which reference the [[URIs]] URI.


Serial No. 09/943,618                          -3-                        RSW920010125US1

1     Claim 11 (currently amended): The method according to Claim 1, wherein at least one of the

2     selected resources [[are]] is a JavaServer Page ("JSP") Pages ("JSPs") and the permitted actions

3     on the at least one resource are methods referenced from the [[JSPs]] JSP.


1     Claim 12 (currently amended): The method according to Claim 1, wherein at least one of the

2     selected resources [[are]] is any resource that is expressible to the security system and the

3     permitted actions on the at least one resource are selected from a set of actions that are permitted

4     on those resources that resource.


1     Claim 13 (currently amended): The method according to Claim 1, wherein the controlling step

2     further comprising comprises the steps of:

3         receiving, from a particular one of the subjects, a an access request for access to a

4     particular one of the actions on a particular one of the selected resources; and

5         permitting the requested access only if the security object created for at least one of the

6     roles granted to the particular subject specifies the particular action on the particular resource.

7     determining one or more roles which are required for accessing the particular resource;

8     determining an identity of a source of the access request;

9     for each of the required roles, until obtaining a successful result or exhausting the

10     required roles, determining whether the identity of the source is associated with the required role;

11     and

12     authorizing access to the particular resource only if the successful result was obtained.

Claim 14 (canceled)

1    Claim 15 (currently amended): A security system for improving security policy administration

2    and enforcement using security objects in a computing network using a role-permission model,

3    comprising:

4        means for associating each of a plurality of roles with one of the security objects, each of

5    the security objects specifying at least one resource and for each resource, at least one action to

6    be permitted on the resource; and

7        means for controlling access, by a plurality of subjects, to the actions on the resources

8    using the security objects, wherein each of the subjects has been granted at least one of the roles.

9    ~~means for identifying one or more groups of permitted actions on selected resources;~~

10   ~~means for assigning a name to each identified group; and~~

11   ~~means for associating subjects with each assigned name.~~


1    Claim 16 (currently amended): The system according to Claim 15, further comprising:

2        means for receiving, from a particular one of the subjects, a ~~an access~~ request for access

3    to a particular one of the actions on a particular one of the ~~selected~~ resources; and

4        means for permitting the requested access only if the security object created for at least

5    one of the roles granted to the particular subject specifies the particular action on the particular

6    resource.

7        ~~means for determining one or more roles which are required for accessing the particular~~

8    ~~resource;~~

Serial No. 09/943,618                          -5-                          RSW920010125US1

9    ~~means for determining an identity of a source of the access request;~~

10   ~~for each of the required roles, until obtaining a successful result or exhausting the~~

11   ~~required roles, means for determining whether the identity of the source is associated with the~~

12   ~~required role; and~~

13   ~~means for authorizing access to the particular resource only if the successful result was~~

14   ~~obtained.~~


1    Claim 17 (currently amended):  A computer program product for ~~improving~~ security policy

2    administration and enforcement <u>in a security system that controls access using security objects,</u> ~~in~~

3    ~~a computing network using a role-permission model,~~ the computer program product embodied on

4    one or more computer readable media and comprising:

5        <u>computer readable program code means for associating each of a plurality of roles with</u>

6    <u>one of the security objects, each of the security objects specifying at least one resource and for</u>

7    <u>each resource, at least one action to be permitted on the resource; and</u>

8        <u>computer readable program code means for controlling access, by a plurality of subjects,</u>

9    <u>to the actions on the resources using the security objects, wherein each of the subjects has been</u>

10   <u>granted at least one of the roles.</u>

11   ~~computer readable program code means for identifying one or more groups of permitted~~

12   ~~actions on selected resources;~~

13   ~~computer readable program code means for assigning a name to each identified group;~~

14   ~~and~~

15   ~~computer readable program code means for associating subjects with each assigned name.~~


Serial No. 09/943,618                     -6-                      RSW920010125US1

1    Claim 18 (currently amended):  The computer program product according to Claim 17, further

2    comprising:

3          computer readable program code means for receiving, from a particular one of the

4    subjects, a an access request for access to a particular one of the actions on a particular one of the

5    selected resources; and

6          computer readable program code means for permitting the requested access only if the

7    security object created for at least one of the roles granted to the particular subject specifies the

8    particular action on the particular resource.

9          computer readable program code means for determining one or more roles which are

10   required for accessing the particular resource;

11   computer readable program code means for determining an identity of a source of the

12   access request;

13   for each of the required roles, until obtaining a successful result or exhausting the

14   required roles, computer readable program code means for determining whether the identity of

15   the source is associated with the required role; and

16   computer readable program code means for authorizing access to the particular resource

17   only if the successful result was obtained.

Serial No. 09/943,618                    -7-                    RSW920010125US1